CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1-48.
- After this Amendment: Claims 1-2, 6-9, 11, 22-24, 28, 31-32, 43, and 46-47

Non-Elected, Canceled, or Withdrawn claims: 3-5, 10, 12-21, 25-27, 29-30, 33-42, 44-45, and 48

Amended claims: 1, 6, 22, 31, and 43

New claims: none

Claims:

1.   **(Currently Amended)** A method comprising:

generating a formal license for content that includes:

  a decryption key for decrypting the content; and

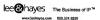 access rules for accessing the content; and

configuring a plurality of license authorities to provide a plurality of partial

licenses, wherein:

  each said license authority provides a respective said partial license;

and

Serial No.: 10/685,234
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

4

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

the plurality of partial licenses are combinable to form the formal license;

wherein the configuring includes:

generating a pre-license from the formal license by encrypting the formal license utilizing an asymmetric encryption algorithm having a public key and a private key, wherein the formal license, the pre-license and the public key are denoted, respectively, as "license", "prel" and "PK" as follows:

$$prel = (license)pk;$$

dividing the private key SK into m partial secret shares according to a (k, m) threshold secret sharing scheme by:

generating a sharing polynomial f(x) ·being represented as follows:

$$f(x) = ao + a1x + ...+ ak-1 xk-1 \quad , \text{ where } ao = SK; \text{ and}$$

calculating each said partial secret share, denoted as Si, for a respective said license authority, denoted by idi, in which i = 1, ..., m, as follows:

$$S_i = f(id_i) \bmod \phi(N),$$ where N is a RSA modulus and $\phi(N)$ is a Euler totient function; and

transmitting the pre-license and a respective said partial secret

Serial No.: 10/685,234
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

5

lee&hayes The Business of IP™
www.leehayes.com 509.324.9256

share to a respective said license authority, wherein each said license authority is configured to generate the respective said partial license from the respective said partial secret share and the pre-license.

2.   **(Original)** A method as described in claim 1, wherein the plurality of partial licenses are provided according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

3.   **(Cancelled)**

4.   **(Cancelled)**

5.   **(Cancelled ; incorporated into claim 1)**

6.   **(Currently Amended)** A method as described in ~~claim 5~~ claim 1, wherein each said license authority verifies the pre-license and the respective

Serial No.: 10/685,234
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

6

lee&hayes   The Business of IP™
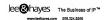www.leehayes.com   509.324.9256

said partial secret share by utilizing a verifiable secret sharing (VSS) scheme in which k public witnesses of the sharing polynomial's $f(x)$ coefficients (denoted as $\{g^{a_0}, \Lambda, g^{a_{k-1}}\}$, where $g \in Z_N^*$) are communicated to each said license authority id_i to verify validity of a respective said partial secret share S_i by determining if the following equation holds:

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot K \cdot (g^{a_{k-1}})^{id_i^{k-1'}} \text{ mod}$$

N.

7. **(Original)** A method as described in claim **1**, further comprising packaging the content to include one or more network addresses that are suitable for locating each said license authority.

8. **(Original)** A method as described in claim **1**, wherein each said license authority is communicatively coupled to a peer-to-peer network.

9. **(Original)** A method as described in claim **1**, wherein the plurality of license authorities are configured based on a consideration such that at least one said license authority provides two or more said partial licenses, wherein the consideration is selected from the group consisting of:

security of the at least one said license authority against unauthorized

Serial No.: 10/685,234
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

7

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

access;

> load sharing of the plurality of license authorities;
>
> availability of each said license authority;
>
> network availability of each said license authority;
>
> hardware resources of each said license authority;
>
> software resources of each said license authority; and
>
> any combination thereof.

10.   (Cancelled)

11.   (Original) One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 1.

12-21. (Cancelled)

22.   (Currently Amended) A method comprising:

obtaining a plurality of partial licenses over a network from a plurality of license authorities, wherein each said partial license is provided, respectively, by a different said license authority; and

> forming a formal license from the plurality of partial licenses, wherein the

formal license includes access rules and a decryption key for accessing content, wherein:

the plurality of partial licenses are obtained from the plurality of license authorities by:

calculating the partial license preli by each said license authority idi from a partial secret share Si and a pre-license prel according to the following equation:

$$prel_i = (prel)^{S_i} \bmod N;$$

generating a random number u to calculate A1 = gu, A2 = prelu, r = u − c * Si, and

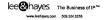$$c = hash\,(g^{S_i}, prel_i, A_1, A_2)\,;\text{ and}$$

communicating the partial license preli, A1, A2, and r by each said license authority; and

the formal license is formed from the plurality of partial licenses by:

determining if k correct partial licenses have been received by validating each said partial license preli by:

calculating

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \bmod N$$

Serial No.: 10/685,234
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

9

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

from public witnesses of a sharing polynomial's coefficients, which are denoted as $\{g^{a_0}, \Lambda, g^{a_{k-1}}\}$, that was utilized to generate the partial secret share Si, where $g \in Z_N^*$, applying $c = hash(g^{S_i}, prel_i, A_1, A_2)$ to calculate c; and checking if $g^r \cdot (g^{S_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$ hold for each said partial license preli, and if so, each said partial license preli is valid; and

combining the plurality of partial licenses to form the formal license, denoted as license, when k valid said partial licenses are obtained, in which:

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)}$$
$$= (prel)^{SK} = ((license)^{PK})^{SK} \mod N,$$

where
$$l_{id_i}(x) = \prod_{j=1, j \neq i}^{k} \frac{x - id_j}{id_i - id_j}.$$

.

23. (Original) A method as described in claim 22, wherein the obtaining includes:

Serial No.: 10/685,234   10
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

examining the content to find a plurality of network addresses of a plurality of license authorities;

requesting the plurality of partial licenses from the plurality of license authorities; and

receiving one or more communications having one or more said partial licenses that are provided by each said license authority.

24.   (Original) A method as described in claim 22, wherein the forming includes combining the plurality of partial licenses to form the formal license.

25.   (Cancelled)

26.   (Cancelled)

27.   (Cancelled; incorporated into claim 22)

28.   (Original) One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 22.

29.   (Cancelled)

30.   (Cancelled)

31.   (Currently Amended) A method comprising:

configuring a plurality of license authorities in a first arrangement to provide a plurality of partial licenses, wherein:

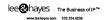each said license authority provides at least one said partial license; and

the plurality of partial licenses are combinable to form a formal license that includes access rules and a decryption key for content; and

updating the first arrangement to form a second arrangement such that:

each said license authority in the second arrangement provides at least one of a plurality of updated partial licenses that are combinable to form the formal license; and

the partial licenses provided in the first arrangement are not combinable with the updated partial licenses to form the formal license;

wherein the updating is performed by:

generating a random (k, m) sharing by each license authority i using a random update polynomial fi, update(x), wherein:

$$f_{i,update}(x) = b_{i,1}x + \ldots + b_{i,k-1}x^{k-1}; \text{ and}$$

Serial No.: 10/685,234
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

12

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

distributing a subshare Si,j by each said license authority i such that each said license authority i has a respective said subshare Si,j from another said license authority wherein:

the subshare $S_{i,j} = f_{i,update}(j)$, $j = 1, \Lambda, m$ is calculated by each said license authority i:

the subshare Si,j is added to the original share S_i of each said license authority to form a new updated share

$$S_i' = S_i + \sum_{j=1}^{m} S_{j,i}$$; and

a new secret sharing polynomial fnew(x) is formed which is a summation of an original polynomial f(x) utilized to generate the plurality of partial licenses in the first arrange and each of the randomly generated polynomials fi,update(x).

32. **(Original)** A method as described in claim 31, wherein the updating is performed periodically.

33. **(Cancelled; incorporated into claim 31)**

34-42. (Cancelled)

Serial No.: 10/685,234
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

13

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

43. **(Currently Amended)** A client device comprising:

a processor; and

memory configured to maintain:

packaged content that includes one or more network addresses that are suitable for locating a plurality of license authorities, wherein each said license authority stores one or more partial licenses;

a content player that is executable on the processor to output content; and

a digital rights management module that is executable on the processor to:

obtain the partial licenses from the plurality of license authorities utilizing the one or more network addresses; and

form a formal license from the obtained partial licenses, wherein the formal license provides access to the packaged content for output by the content player;

obtain the partial licenses from the plurality of license authorities, wherein each said license authority provide a respective said partial license by:

calculating the partial license $prel_i$ by each said license authority id_i from a partial secret share S_i and a pre-license $prel$ according to the following equation:

Serial No.: 10/685,234
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

14

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

$$prel_i = (prel)^{S_i} \bmod N;$$

generating a random number u to calculate A1 = gu, A2 = prelu, r = u − c * Si, and

$$c = hash\,(g^{S_i}, prel_i, A_1, A_2)\,;\text{ and}$$

communicating the partial license preli, A1, A2, and r by each said license authority; and

the formal license is formed from the plurality of partial licenses by:

determining if k correct partial licenses have been received by validating each said partial license preli by:

calculating

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \bmod N$$

from public witnesses of a sharing polynomial's coefficients, which are denoted as $\{g^{a_0}, \Lambda, g^{a_{k-1}}\}$, that was utilized to generate the partial secret share Si, where $g \in Z_N^*$,

applying $c = hash\,(g^{S_i}, prel_i, A_1, A_2)$ to calculate c; and

Serial No.: 10/685,234
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

15

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

checking if $g^r \cdot (g^{s_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$ hold for each said partial license preli, and if so, each said partial license preli is valid; and

combining the plurality of partial licenses to form the formal license, denoted as license, when k valid said partial licenses are obtained, in which:

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)}$$
$$= (prel)^{SK} = ((license)^{PK})^{SK} \bmod N,$$

where $$l_{id_i}(x) = \prod_{j=1, j \neq i}^{k} \frac{x - id_j}{id_i - id_j}.$$

44.   (Cancelled)

45.   (Cancelled)

46.   (Original) A client device as described in claim 43, wherein the one or more network addresses include a proxy address for locating a network address of each said license authority.

Serial No.: 10/685,234   16
Atty Docket No.: MS1-1753US
Atty/Agent: Kasey C. Christie
RESPONSE TO NON-FINAL OFFICE ACTION

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

47.   **(Original)** A client device as described in claim 43, wherein the one or more network addresses include a network address of each said license authority.

48.   **(Cancelled; incorporated into claim 43)**